

REMARKS

In the Office Action of May 1, 2007, Claims 1-4 were rejected under 35 U.S.C. § 102(b) as being anticipated by White et al., "Anatomy of a Commercial-Grade Immune System," <<http://citeseer.ist.psu.edu/white99anatomy.html>> 1999 (hereinafter "White"). Claims 5-16 are newly added.

Pursuant to 37 C.F.R. § 1.111 and for the reasons set forth below, applicants respectfully request reconsideration and allowance of the pending claims. Prior to discussing the reasons why applicants believe that the pending claims are in condition for allowance, brief summaries of the claimed subject matter and the cited and applied reference, White, are presented. However, while the brief summaries are presented to assist the Examiner to appreciate the differences between the claimed subject matter and the cited reference, they should not be viewed as limiting upon the disclosed subject matter.

Brief Description of Claimed Subject Matter

In order to better appreciate the differences between the claimed subject matter and other anti-virus systems, including White, most anti-virus software recognizes viruses according to a "signature" computed/derived from the malware itself. In a general sense, when a suspected file arrives, a hash (which yields fairly unique results over a corpus body of files) is generated of that suspected file. The resulting hash value is then compared to hash values of known malware, and if there is match, the suspected file is therefore malware. The problem with this type of identification is twofold: (1) for a hash to generate relatively unique results over a corpus body of files, small modifications to a file will result in a different hash value; and (2) malware exploits this by being self-polymorphic, i.e., it has the ability to modify itself without changing its underlying function to the end that it cannot be recognized according to a hash value/signature based on the file itself. The claimed subject matter addresses these issues.

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

The claimed subject matter is generally directed to determining whether a code module represents malware (i.e., a virus, worm, Trojan horse, etc.) according to behaviors of the code—the underlying behaviors—and not a hash value of the code. In this way, polymorphic malware cannot simply change its outward appearance and escape detection.

According to the claimed subject matter, when a code module is received, a behavior evaluation module is selected that corresponds to the particular code module. The code module is then executed within the selected behavior evaluation module. Executing the code module exposes the underlying behavior of the malware. As the code module is executing, some of the behaviors/actions that the code module makes are recorded. The recorded behaviors are then compared to recorded behaviors of known malware to determine whether there is a match, i.e., that the code module is known malware.

Additional aspects of the claimed subject matter include, for each behavior evaluation module, a predefined set of behaviors to record if/when they occur. Moreover, in one embodiment, the predefined set of behaviors corresponds to a predefined set of system calls that are viewed as "interesting", i.e., a behavior (system call) worthy of recording in a behavior signature.

In sum, the claimed subject matter is directed to identifying malware according to its underlying functionality, i.e., according to its exhibited behaviors. No other system matches malware according to what the malware does. Instead, other systems identify a suspected file as malware according to a signature derived from the suspected file.

Brief Description of White

White describes a system for discovering new viruses, creating a "cure" for the new virus, as well as a signature for future identification. However, in the process of discovering new viruses, White explicitly describes that it first tries to identify a file as malware (or as a clean

file) according to a checksum of the file. More particular, the file is submitted to an Administrator system that generates a checksum (signature) of the file and compares that value to values of files known to be clean and files known to be malware. White, pg. 14. If the file is cannot be determined to be a clean file or malware, it is forwarded to a gateway where the latest virus definitions are found and the signature is again checked for malware or clean file. Only when the file has not been previously identified is the file delivered to the analysis center. At the analysis center, the file is executed on several virtual systems so that a sufficient analysis of the results of the infection can be determined, as found in "goat" files. White, pg. 21. Analysis is performed and a definition file is generated. The definition file includes a signature string (*id.*) and information such that infected files can be returned to their original state.

It should be noted that White states that the virtual environments can be instrumented "so that the analysis center can sense what the virus is doing as it does it." White, pg. 21. However, whether or not the analysis center senses what the virus does as it is doing it, nothing in White discloses recording some of the behaviors during execution of the code module and then comparing the recorded behaviors against recorded behaviors of known malware to identify/determine the code module as malware.

35 U.S.C. § 102(b) Rejections

Claim 1

The Office Action asserts that White discloses each and every element of Claim 1. Applicants respectfully disagree. Applicants submit that White fails to disclose:

each dynamic behavior evaluation module **records some execution behaviors of the code module as it is executed**, wherein the execution behaviors of the code module are recorded into a behavior signature corresponding to the code module; and

a behavior signature comparison module that **obtains the behavior signature and compares the behavior signature to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited execution behaviors of the code module match the exhibited execution behaviors of known malware.** (Emphasis added.)

As discussed above, White is directed to, first, determining if a suspect file is known as either a clean file or as malware according to a signature determined from the file itself (not from its exhibited behaviors during execution). If the file is not known (as malware or not), it is ultimately passed to the analysis center where it is run in virtual environments on several different machines with the intent that "goat" files are infected, with the goal to "obtain enough virus samples to permit analysis." White, pg. 21. The samples are analyzed involving "extracting a good signature string for the virus" and creating disinfection information. *Id.* In all of this, White completely fails to disclose recording some execution behaviors of the code module as it executes, and comparing the recorded execution behaviors of the code module to execution behaviors of known malware.

In light of the amendments to Claim 1 and in view of the remarks above, applicants submit that White fails to disclose each and every element of Claim 1. A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987). Accordingly, applicants submit that the 35 U.S.C. § 102(b) rejection of Claim 1 should be withdrawn and the claim allowed.

Claim 2

Applicants point out that, while differing in scope, independent Claim 2 recites substantially similar elements to those found in independent Claim 1, including elements not found in White. In particular, Claim 2 recites:

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

wherein each dynamic behavior evaluation module **records some execution behaviors of the code module as it is executed**, wherein the execution behaviors of the code module are recorded into a behavior signature corresponding to the code module; and

a behavior comparison means for **comparing the behavior signature to the known malware behavior signatures in the storage means to determine whether the exhibited execution behaviors of the code module match the exhibited execution behaviors of known malware**. (Emphasis added.)

In this light, applicants submit that the arguments set forth in regard to Claim 1 are equally applicable in regard to Claim 2, that Claim 2 is in condition for allowance, and request that the 35 U.S.C. § 102(b) rejection of this claim be withdrawn and the claim allowed.

Claims 3 and 4

Applicants point out that, while differing in scope, independent Claims 3 and 4 recite similar elements to those found in independent Claim 1, including elements not found in White. In particular, Claims 3 and 4 include the following:

recording some execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module during execution of the code module; and

comparing the recorded execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware execution behaviors.

In this light, applicants submit that the arguments set forth in regard to Claim 1 are equally applicable in regard to independent Claims 3 and 4, that Claims 3 and 4 are in condition for allowance, and request that the 35 U.S.C. § 102(b) rejections of these claims be withdrawn and the claims allowed.

CONCLUSION

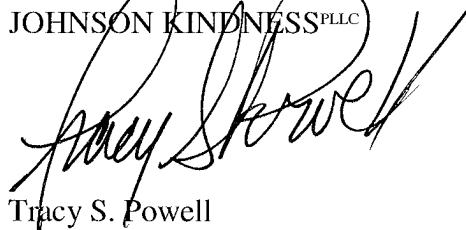
In view of the above amendments and remarks, applicants respectfully submit that the present application is in condition for allowance. Reconsideration and reexamination of the

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

application, and allowance of the claims at an early date, are solicited. If the Examiner has any questions or comments concerning the foregoing response, the Examiner is invited to contact the applicants' undersigned attorney at the number below.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^{PLLC}

A handwritten signature in black ink, appearing to read "Tracy S. Powell", is written over the printed name and firm name.

Tracy S. Powell
Registration No. 53,479
Direct Dial No. 206.695.1786

TSP:lal

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100